

AF
FTW

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10991268-3

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Richard M. Butler
Application No.: 10/686,331
Filing Date: October 14, 2003

Confirmation No.: 7201
Examiner: Do, Chat C.
Group Art Unit: 2193

Title: GENERATION OF CRYPTOGRAPHICALLY STRONG RANDOM NUMBERS USING MISRS

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on November 18, 2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

(a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

1st Month \$120 2nd Month \$450 3rd Month \$1020 4th Month \$1590

The extension fee has already been filed in this application.

(b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: November 18, 2005

OR

I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name: Chasity C. Rossum

Signature: Chasity C. Rossum

Respectfully submitted,

Richard M. Butler

By: Gregory W. Osterloth

Gregory W. Osterloth

Attorney/Agent for Applicant(s)

Reg No. : 36,232

Date : November 18, 2005

Telephone : (303) 291-3204



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Appl. No. : 10/686,331 Confirmation No. 7201
Appellant : Richard M. Butler
Filed : October 14, 2003
TC/A.U. : 2193
Examiner : Do, Chat C.

Docket No. : 10991268-3

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
PO Box 1450
Alexandria VA 22313-1450

APPEAL BRIEF

Table of Contents

Section:

| | |
|--|-----|
| Table of Contents..... | i |
| Real Party in Interest..... | 2 |
| Related Appeals and Interferences..... | 3 |
| Status of Claims..... | 4 |
| Status of Amendments..... | 5 |
| Summary of Claimed Subject Matter..... | 6 |
| Grounds of rejection to be Reviewed on Appeal..... | 7 |
| Argument..... | 8 |
| Claims Appendix..... | A-1 |
| Evidence Appendix..... | B-1 |
| Related Proceedings Appendix..... | C-1 |



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Appl. No. : 10/686,331 Confirmation No. 7201
Appellant : Richard M. Butler
Filed : October 14, 2003
TC/A.U. : 2193
Examiner : Do, Chat C.

Docket No. : 10991268-3

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
PO Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF

Dear Sir:

This Appeal Brief is submitted in response to the Examiner's Final Office Action dated September 23, 2005.

Appellants filed a Notice of Appeal with this Appeal Brief, on November 18, 2005.

11/22/2005 EFLDRES 00000022 082025 10686331

01 FC:1402 500.00 DA

Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, Texas 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, California. The general or managing partner of HPDC is HPQ Holdings, LLC.

Appl. No. 10/686,331
Appeal Brief dated Nov. 18, 2005
Reply to Final Office Action of Sep. 23, 2005

Related Appeals and Interferences

There are no related appeals and/or interferences.

Appl. No. 10/686,331
Appeal Brief dated Nov. 18, 2005
Reply to Final Office Action of Sep. 23, 2005

Status of Claims

Claims 1-22 are pending, all of which stand rejected and are appealed. A copy of the claims is attached as a Claims Appendix to this Appeal Brief.

Appl. No. 10/686,331
Appeal Brief dated Nov. 18, 2005
Reply to Final Office Action of Sep. 23, 2005

Status of Amendments

All amendments have been entered.

Summary of Claimed Subject Matter

In a first embodiment (claim 1), a method (p. 13, par. [0034]; FIG. 1, 100) of generating a random number comprises 1) retrieving (FIG. 1, 102) values from a number of multiple input shift registers (MISRs) (p. 13, par. [0037] - p. 16, par. [0041]; FIG. 4, 402-412) which are coupled to a number of microprocessor buses (FIG. 4, 414-424); and 2) generating (FIG. 1, 104) a random number which is based on the values retrieved from the number of MISRs.

In a second embodiment (claim 22), a method of generating an encryption key (FIG. 10, 1012) comprises 1) assigning (p. 22, par. [0059]; FIG. 9, 900) a built-in self-test (BIST) local block of a microprocessor a major address; 2) assigning (p. 22, par. [0059]; FIG. 9, 902) each of a number of multiple input shift registers (MISRs; FIG. 4, 402-412) in the BIST local block a minor address; 3) issuing (p. 22, par. [0060]; FIG. 9, 904) an instruction to turn on and initialize the MISRs; 4) issuing (pp. 22-23, par. [0061]-[0062]; FIG. 9, 908) a request to read the MISRs, in response to a request for an encryption key; and 5) XORing (p. 22, par. [0061]; FIG. 9, 910) the MISR readings with each other, and with historical readings, if any, to generate an encryption key.

Grounds of Rejection to be Reviewed on Appeal

I. Whether claims 1, 2 and 7-21 should be rejected under 35 USC 103(a) as being unpatentable over Edelkind et al. (US Pat. No. 5,987,483) in view of Nozuyama (US Pat. No. 5,867,409).

II. Whether claims 3-6 should be rejected under 35 USC 103(a) as being unpatentable over Edelkind et al. (US Pat. No. 5,987,483) in view of Nozuyama (US Pat. No. 5,867,409) and Thomlinson et al. (US Pat. No. 5,778,069).

III. Whether claim 22 should be rejected under 35 USC 103(a) as being unpatentable over Nozuyama (US Pat. No. 5,867,409) in view of Edelkind et al. (US Pat. No. 5,987,483).

Argument

I. Whether claims 1, 2 and 7-21 should be rejected under 35 USC 103(a) as being unpatentable over Edelkind et al. (US Pat. No. 5,987,483; hereinafter “Edelkind”) in view of Nozuyama (US Pat. No. 5,867,409).

a. Claims 1, 2, 7-9, 11, 12, 17 & 19-21

Claim 1 recites:

1. A method of generating a random number, comprising:
retrieving values from a number of multiple input shift registers (MISRs) which are coupled to a number of microprocessor buses; and
generating a random number which is based on the values retrieved from the number of MISRs.

With respect to claim 1, the Examiner asserts that Edelkind teaches all of the elements of appellant’s claim in FIG. 2, but for the values on which a random number is based being retrieved from “a number of multiple input shift registers”. The Examiner also asserts that:

. . . Nozuyama discloses in Figure 2 random number generator is a MISR. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to replace a multiple random number generators with a multiple MISRs as disclosed in Nozuyama’s Figure 2 into Edelkind et al.’s Figure 4 because it would enable to increase the randomness and performance of the system random output.

9/23/2005 Final Office Action, sec. 4, pp. 2-3.

Appellant respectfully disagrees. To begin, Edelkind not only fails to teach retrieving values from a number of MISRs (as the Examiner admits), but Edelkind also fails to teach that a MISR, or any other element that might collect a value from which a random number could be based, is “coupled to a number of microprocessor buses”. Rather, Edelkind teaches that a “spatially resolved random number

generator 200” comprises “radiation detectors” for acquiring input for a random number generator. A radiation detector is quite different from a microprocessor bus.

Although Nozuyama does disclose a MISR, Nozuyama does not disclose or suggest that one or more MISRs should be “coupled to a number of microprocessor buses” for the purpose of random number generation.

If the Examiner’s rejection of claim 1 is to be sustained, one of ordinary skill in the art would have had to find it obvious to replace Edelkind’s “radiation detector” with an element that is structurally and functionally different - i.e., a MISR. This person of ordinary skill in the art would then have had to jump to the conclusion that a good way to “seed” the MISR would be to couple it to a microprocessor bus - which bus, in the context of Edelkind’s disclosure, wasn’t even significant enough to be assigned a reference number. It is appellant’s opinion that one of ordinary skill in the art would not have found the above steps “obvious”.

Due to the deficiencies of both Edelkind and Nozuyama, appellant’s claim 1 is believed to be allowable. Claims 2 and 7-9, 11, 12, 17 and 19-21 are believed to be allowable at least for the reason that they depend from claim 1.

b. Claim 10

Claim 10 recites:

10. The method of claim 1, wherein generating a random number comprises hashing together the values retrieved from the number of MISRs.

With respect to claim 10, the Examiner asserts that Edelkind teaches that, “generating a random number comprises hashing together the values retrieved from the number of MISRs (300).” See, 9/23/05 Final Office Action, sec. 4, p. 4. Appellant respectfully disagrees.

Edelkind makes absolutely no mention of “hashing” values together. Although Edelkind discloses a “combiner 300”, Edelkind does not indicate that the combiner

300 performs any sort of hashing. Rather, Edelkind indicates that the combiner 300 may be, for example, a “multiplexer” that can be “controlled to select for output the random number sequences in any manner to generate a random number sequence therefrom.” See, Edelkind, col. 5, lines 52-55. In appellant’s opinion, sandwiching a plurality of values together in a selected order bears no resemblance to “hashing” a plurality of values together.

Appellant’s claim 10 is believed to be allowable at least for the reason that it depends from claim 1, and for the above additional reason.

c. Claims 13-16

Claim 13 recites:

13. The method of claim 1, wherein values are retrieved from the number of MISRs via an operating system call.

With respect to claim 13, the Examiner asserts that Edelkind teaches that, “values are retrieved from the number of MISRs via an operating system call (310 and col. 5 lines 47-50).” See, 9/23/05 Final Office Action, sec. 4, p. 4. Appellant respectfully disagrees.

Edelkind teaches that a random number is output from a “combiner 300”, and that the combiner may be controlled by a “microprocessor or computer, for example, that is controlled by a software program”. See, Edelkind, col. 5, lines 46-55. As disclosed in appellant’s Specification, one way to retrieve a random number is at the request of an application program. However, appellant also indicates that it is more preferable to obtain a random number using an operating system call, and that the operating system call is preferably of the highest privilege level. In this manner, the random number source (i.e., a MISR) will be more difficult to seed and/or monitor (e.g., for purposes of attack). Edelkind fails to provide any teaching or suggestion in this regard, and only states that the “combiner 300” may be read by a

microprocessor under control of an “application program”. An “application program” is not equivalent to an “operating system”.

Appellant’s claim 13 is believed to be allowable at least for the reason that it depends from claim 1, and for the above additional reason. Claims 14-16 are believed to be allowable at least for the reason that they depend from claim 13.

d. Claim 18

Claim 18 recites:

18. The method of claim 1, wherein generating said random number comprises providing the values retrieved from the number of MISRs, as well as historic values retrieved from the number of MISRs, to a pseudo-random number generator.

With respect to claim 18, the Examiner does not indicate where Edelkind or Nozuyama teach the limitations of this claim. Claim 18 indicates that “values retrieved from the number of MISRs” and “historic values retrieved from the number of MISRs” are provided to a pseudo-random number generator. Note that this is not a claim to a MISR’s inherent operating characteristics, but is instead a claim to multiple values being read from a MISR and combined externally to the MISR (e.g., using a pseudo-random number generator).

Appellant’s claim 18 is believed to be allowable at least for the reason that it depends from claim 1, and for the above additional reason.

II. Whether claims 3-6 should be rejected under 35 USC 103(a) as being unpatentable over Edelkind et al. (US Pat. No. 5,987,483; hereinafter "Edelkind") in view of Nozuyama (US Pat. No. 5,867,409) and Thomlinson et al. (US Pat. No. 5,778,069; hereinafter "Thomlinson").

With respect to claims 3-6, the Examiner admits that Edelkind and Nozuyama do not disclose the additional limitations of these claims. See, 10/26/2004 Office Action, p. 7, sec. 8. However, the Examiner asserts that:

. . . Thomlinson et al. disclose in Figure 3 (col. 3 lines 15-30) that the input data can be anything from the static bits (52), machine bits (54), and application bits (56). Therefore, it would have been obvious application to a person having ordinary skill in the art at the time the invention is made to input a data, address, instruction data, or instruction address as the input data to one of number MISRs as disclosed in Thomlinson et al.'s invention into Edelking [sic] et al. in view of Nozuyama's invention because it would increase the randomness for generating a random number from multiple random sources (col. 3 lines 30-35).

9/23/2005 Final Office Action, sec. 5, pp. 6-7.

Appellant respectfully disagrees. Thomlinson states:

The input device also gathers one or more external classes of bits from one or more sources external to the random number generator. For instance, in the preferred implementation, the input device gathers a machine class of bits which relate to operating parameters of the computer (e.g., time of day, date, memory allocation) and an application class of bits which relate to execution of an application running on the computer. In this last class, the application supplies the bits to the random number generator. One example of an application class of bits is a set of bits produced by monitoring keystroke frequency as the user types in a message. The input device concatenates the three classes of bits into an arbitrary length input bit string.

Thomlinson, col. 3, lines 16-28.

Thus, Thomlinson does not teach that a MISR derives a random number seed from any sort of microprocessor bus. Rather, Thomlinson teaches that a "machine class of bits" may be obtained from "operating parameters of the computer (e.g., time of day, date, memory allocation)" or an "application class of bits" that relate to

“execution of an application running on [a] computer”, such as a set of bits produced by monitoring keystroke frequency”.

An “operating parameter” of a computer is not equivalent to a “microprocessor bus”. And, although the state of a microprocessor bus may be influenced by user keystrokes, a “keystroke” or other byproduct of running an “application” is not equivalent to a “microprocessor bus”.

Appellant’s claims 3-6 are believed to be allowable at least for the reason that they depend from claim 1 (see arguments of Section I, *supra*), and for the above additional reason.

III. Whether claim 22 should be rejected under 35 USC 103(a) as being unpatentable over Nozuyama (US Pat. No. 5,867,409) in view of Edelkind et al. (US Pat. No. 5,987,483; hereinafter “Edelkind”).

With respect to appellant’s claim 22, the Examiner asserts that:

. . . Nozuyama discloses in Figures 3 and 7 a method of generating a random number comprising: assigning a built-in self-test (BIST) (col. 1 lines 35-40) local block of a microprocessor a major address (d_0 - d_{n-1} in Figure 3), assigning each of a number of multiple input shift registers (MISRS) in the BIST local block a minor address (each individual data d_x). . . it would have been obvious to a person having ordinary skill in the art at the time the invention is made to use the random number in encryption key as disclosed in Edelkind et al.’s invention into Nozuyama’s invention because it would enable to prevent detectable key.

9/23/2005 Final Office Action, sec. 6, p. 7.

Appellant respectfully disagrees. Although Nozuyama teaches that an LFSR may be used to compress data obtained from a device under test (DUT), Nozuyama contains absolutely no discussion of assigning a BIST local block a major address, or assigning minor addresses to MISRs in the BIST local block. Nor does Nozuyama indicate why one would want to do so. Furthermore, the data sampled by Nozuyama’s LFSR is not intended to be random, but is rather expected to match that which is expected, to thereby aid in testing/verifying the operation of a DUT. It is

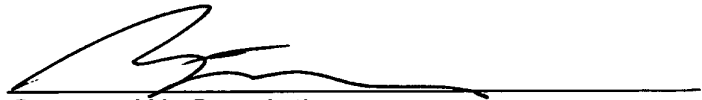
therefore a huge leap, and one that is not supported by Nozuyama's teachings, to assert that it would have been obvious to substitute Nozuyama's LFSR for Edelkind's radiation detectors to thereby create a better random number generator. Appellant's claim 22 is therefore believed to be allowable.

IV. Conclusion

In summary, the art of record does not teach nor suggest the subject matter of Appellant's claims 1-22. These claims are therefore believed to be allowable.

Respectfully submitted,
DAHL & OSTERLOTH, L.L.P.

By:


Gregory W. Osterloth
Reg. No. 36,232
Tel: (303) 291-3200

Claims Appendix

1. A method of generating a random number, comprising:
retrieving values from a number of multiple input shift registers (MISRs) which are coupled to a number of microprocessor buses; and
generating a random number which is based on the values retrieved from the number of MISRs.
2. The method of claim 1, wherein the number of MISRs is one.
3. The method of claim 1, wherein one of the number of MISRs is coupled to a data bus which transfers data between a data cache and a CPU core.
4. The method of claim 1, wherein one of the number of MISRs is coupled to a data address bus which transfers data addresses between a data address cache and a CPU core.
5. The method of claim 1, wherein one of the number of MISRs is coupled to an instruction data bus which transfers instructions between an instruction data cache and a CPU core.
6. The method of claim 1, wherein one of the number of MISRs is coupled to an instruction address bus which transfers instruction addresses between an instruction address cache and a CPU core.
7. The method of claim 1, wherein one of the number of MISRs is coupled to a bus which runs wholly within an integrated circuit package.
8. The method of claim 1, wherein retrieving values from the number of MISRs comprises:
loading bits of a value stored in a first of the number of MISRs, in parallel, into a

temporary register; and

retrieving the value stored in the temporary register.

9. The method of claim 1, wherein retrieving values from the number of MISRs comprises retrieving a value from a first of the number of MISRs by stepping the first of the number of MISRs to serially shift a plurality of bits out of the MISR.

10. The method of claim 1, wherein generating a random number comprises hashing together the values retrieved from the number of MISRs.

11. The method of claim 1, wherein generating a random number comprises XORing the values retrieved from the number of MISRs.

12. The method of claim 1, further comprising turning on and initializing each of the number of MISRs upon boot of a computer in which the MISRs reside.

13. The method of claim 1, wherein values are retrieved from the number of MISRs via an operating system call.

14. The method of claim 13, wherein said operating system call is of a highest privilege level.

15. The method of claim 13, wherein generating a random number is performed immediately after the number of MISR readings are taken, the method further comprising storing the random number in a temporary location for subsequent use.

16. The method of claim 13, wherein said operating system call is issued in response to an application's request for a random number.

17. The method of claim 1, wherein retrieving values from a number of MISRs comprises a computer program's issuance of a request to read the number of

MISRs.

18. The method of claim 1, wherein generating said random number comprises providing the values retrieved from the number of MISRs, as well as historic values retrieved from the number of MISRs, to a pseudo-random number generator.

19. The method of claim 1, further comprising testing the number of MISRs by:
 - initializing the number of MISRs to known values;
 - executing a test program on the microprocessor in which the number of MISRs reside;
 - retrieving values from the number of MISRs;
 - comparing the values retrieved from the number of MISRs with expected values; and
 - indicating a failure of one of the number of MISRs if its retrieved value does not agree with its expected value.

20. The method of claim 1, wherein the random number is an encryption key.

21. The method of claim 1, wherein the MISRs form part of a microprocessor's built-in self-test hardware.

22. A method of generating an encryption key, comprising:
 - assigning a built-in self-test (BIST) local block of a microprocessor a major address;
 - assigning each of a number of multiple input shift registers (MISRs) in the BIST local block a minor address;
 - issuing an instruction to turn on and initialize the MISRs;
 - issuing a request to read the MISRs, in response to a request for an encryption key;
 - XORing the MISR readings with each other, and with historical readings, if any, to generate an encryption key.

Appl. No. 10/686,331
Appeal Brief dated Nov. 23, 2005
Reply to Final Office Action of Sep. 23, 2005

Evidence Appendix

None.

Appl. No. 10/686,331
Appeal Brief dated Nov. 23, 2005
Reply to Final Office Action of Sep. 23, 2005

Related Proceedings Appendix

None.